PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00 | A1

(11) International Publication Number: WO 99/50734

(43) International Publication Date: 7 October 1999 (07.10.99)

(21) International Application Number: PCT/US99/05025

(22) International Filing Date: 8 March 1999 (08.03.99)

(30) Priority Data:
09/052,844 31 March 1998 (31.03.98) US

(71) Applicant: AT & T CORP. [US/US]; 32 Avenue of the Americas, New York, NY 10013–2412 (US).

(72) Inventors: GOLDBERG, Randy, G.; 48 Primrose Circle, Princeton, NJ 08540 (US). ROSEN, Kenneth, H.; 107 Red Hill Road, Middletown, NJ 07748 (US). SALIMANDO, Steven, Charles; 22 N. Rivers Edge Drive, Little Silver, NJ 07739 (US).

(74) Agents: DWORETSKY, Samuel, H. et al.; AT & T CORP., P.O. Box 4110, Middletown, NJ 07748 (US).

(81) Designated States: BR, CA, CN, JP, MX, NO, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: A METHOD OF AND APPARATUS FOR COMPUTER SECURITY USING A TRANSMITTING LOCATION DEVICE

(57) Abstract

A method and apparatus enhance computer security based on pre–registration and tracking of a computer user's location. A location device accompanies an individual attempting to log–in to a computer network from a location distant to the network. When the location device is activated, it transmits a location signal which is received by the computer network. The network then determines from the location signal where the individual is located during the log–in process. If the individual is at a pre–defined physical location, the computer grants access; otherwise, access is denied.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

A METHOD OF AND APPARATUS FOR COMPUTER SECURITY USING A TRANSMITTING LOCATION DEVICE

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention relates to a method of and apparatus for computer security using a transmitting location device, and, more particularly, to a method of and apparatus for adding an additional layer of computer security based on registration and tracking of the computer user's location.

DESCRIPTION OF RELATED ART

The increasing use of remote access, that is the use of a computer or other device to communicate with a computer network from a location distant from the network, has enabled individuals who otherwise do not have authorized access to the computer network to none-the-less violate computer security from afar. The ability of computer hackers to infiltrate a computer network from a distant location can be a serious threat to a company's well-being. This threat is especially serious for companies which have an ever increasing reliance on a workforce who tele-commute to work from home everyday. Thus knowing where an individual is when they attempt to gain entry to the computer network would be an important aspect of computer security.

Position detection for locating individuals, devices, and vehicles has been accomplished. For example, U.S. Patent No. 5,689,269, issued November 18, 1997 to Norris, relates to an apparatus and method for determining the position of a first device relative to the position of a second device using the Global Positioning System (GPS). The first device, with a person or object to be located, transmits telemetry position data to the second device after first receiving a GPS signal and determining its own location using that GPS signal. The second device receives

the telemetry position data from the first device and calculates a relative distance between the two devices. The calculation performed by the second device is based on the telemetry position data received from the first device and knowledge about its own position determined from GPS signals that it has previously received. The second device is also capable of determining direction and difference in elevation between the first and second devices.

Further, U.S. Patent No. 5,550,551, issued August 27, 1996 to Alesio, relates to a position monitoring system and method particularly applicable to vehicle monitoring. When activated, a position detector mounted on the vehicle uses GPS signals to determine vehicle location information. On a pre-determined basis, the position detector periodically updates the vehicle location information and transmits a location information signal based on the vehicle's location to a remote dispatch center. The dispatch center receives the transmitted location information signal from the position detector, determines the vehicle location, and relays that information to an appropriate law enforcement agency.

Yet another example, U.S. Patent No. 5,389,934, issued February 14, 1995 to Kass, relates to a portable system for locating a person, vehicle or object. The system uses a GPS unit and a piece of cellular telephone equipment. The system's locating function is first activated by receipt of a telephone call on the piece of cellular telephone equipment. Upon this activation, the system then determines its own location via the GPS unit and responds to the call with a voice message stating its current location. The person, vehicle or object may then be retrieved.

As can be seen, however, while the ability to accurately locate a person, device or vehicle exists, this ability has not been applied to help with computer security. As the threat of a breach of computer security from afar still exists, and in fact seems to be increasing, there still remains a need for a method of enhancing computer security based on detection of location.

SUMMARY OF THE INVENTION

Accordingly, in response the present invention, as embodied and broadly described herein, provides a method of and apparatus for adding an

additional layer of security to the computer log-in process based on registration and detection of location. Thus, an individual who wishes to log-in to a computer system must not only be an authorized user of the system, but must also be attempting to log-in from a pre-registered and authorized location or zone.

Proper location is checked through the use of a transmitting location device. When an individual who is an authorized user of a computer network desires to access that network from a location distant to the network, a location device is activated. Once activated, the location device will transmit a location signal to the computer network.

An additional layer of security is thus added through the use of the transmitting location device. This is accomplished when the individual is logging-in to the network. Once the locating device has been activated and is transmitting a locating signal, the computer network will receive that locating signal and determine where the individual is as they are attempting to log-in. The computer network will then match that determined location against a list of pre-registered locations. If the individual is in fact located at a location that has been pre-registered, the computer network will allow access using both the location information and the standard security measures (e.g. ID and password). Thus not only must the person be an authorized user (which can be determined by the ID and passcode, inter alia), but the location must be a pre-authorized and pre-registered location.

Further, the additional security may be added to the on-going session as well. As the individual is logged-on to the network, the network may reactivate the location device to periodically check the individual's location. Periodic updates allow the computer network to ensure that the individual is still at and/or in the pre-registered location or zone, and that a proper location signal is being received.

The present invention, including its features and advantages, will become more apparent from the following detailed description with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a flow chart of a method of enhancing computer security using a transmitting location device in which the location device transmits a location signal during an attempt to log-in to a secure computer network, according to an embodiment of the present invention.

Figure 2 illustrates a schematic of an apparatus by which transmission of the location signal from the location device to the computer network can be carried out, according to an embodiment of the present invention.

DETAILED DESCRIPTION

Figures 1 and 2 show a method and an apparatus for adding an additional layer of security to a computer log-in process based upon a pre-registration operation and a subsequent detection of a computer user's location. Thus the location from which the computer user attempts to log-in, and from which he or she continues to work, becomes an additional element by which computer security may be maintained. If the individual using the computer logs-in from a pre-registered location, and the central computer recognizes that location as an authorized location, log-in to the computer network is permitted. However, if the identified location is determined not to be an authorized location, log-in is not permitted. Subsequent updates of the computer user's location can also be used to ensure that the user is still in the authorized location. Thus if the individual is subsequently determined to be outside of the pre-registered location, access to the computer network can be terminated.

An individual who will have need of logging-in to a computer network from a location outside of the immediate area of the computer network will be required to pre-register the location (or locations) from which he or she shall be logging-in. A central computer will then consider each pre-registered location as an authorized location for that individual. In essence, then, the location is keyed to that individual and is the only location from which the individual may log-in and continue to work. Approval of the location by the central computer may be dependent upon any number of pre-set criteria. Further, ultimate approval may reside with the appropriate company personnel. It is to be understood, then, that

the location approval process may be established and administered in any manner which the company (and/or individuals) using the present invention approves. It is not to be limited to simply the embodiment herein described, and is only of importance in ensuring that the registered locations are in fact pre-approved.

The actual locations being pre-registered by the computer user may be a single place or a broader area. For instance, an individual may want to pre-register his or her home, and may also want to pre-register the area which follows a route to and from work. Such a registration scheme thus allows the individual to work from home and also to work while en route to or from work. It is to be understood, of course, that the number of locations which each individual may be allowed to register can be pre-set. Further, registration of places or areas may be keyed to specific days or to specific times of the day. An individual may want to register his or her home only for authorized use during the weekends, when that individual knows he or she may need to work from home. The route to and from work may be registered for those times of the day which the user knows he or she is more likely to be commuting. Even further, if the user knows that he or she will be traveling away on business, the user may pre-register the location to which he or she will be traveling, and may register for only those days on which he or she expects to actually be there.

Detection of the individual's actual location when he or she attempts to log-in to a computer network is accomplished by activation and tracking of a locating device which the individual shall have with them. The individual may either be personally carrying the locating device, or it may be attached to, or an integral part of, the computer terminal (whether portable or fixed) from which the individual is logging-in. The locating device itself is a transmitting and receiving device capable of both sending and receiving a location signal. The transmission of the locating signal may, of course, be continuous or intermittent, and may be digital and/or analog in nature.

Activation and initial tracking of the locating device is triggered by the central computer of the network at the time of log-in. Further explanation of the activation and tracking sequence will be given below with reference to the drawings.

Referring to Figure 1, a central computer may have associated with it a network, which from the central computer's perspective is co-located with that computer. In step 100 an individual who will have a need to log-in to the central computer from a site remote from or not co-located with the central computer will pre-register one or more locations from which he or she will want to log-in. Registration of such log-in sites will preferably occur at the location of the central computer using a controller that interfaces with the central computer. Alternatively, such registration may be accomplished from a secure remote site. Once the sites for remote access have been input to the central computer, in step 110 an approval process for each location input will be implemented. As stated above, there may be various approval processes. Preferably someone having a position of authority and/or responsibility for overseeing computer security will give final approval for remote access sites. Further, each site may be designated as "dormant" until an attempt to log-in is made from that remote site. Once a log-in occurs from a site, the site's status may be changed to "active" and notification of the log-in and use of the site may be sent to the appropriate persons (i.e., persons in charge of computer security), and perhaps including the site's registrant. Further, an "active" site which has not been used for a pre-set period of time may be changed back to a "dormant" state. Such classification of sites can be helpful in keeping track of which sites have and/or have not been used and may further help to maintain security.

Once a log-in location has been pre-registered and approved, an individual may access the central computer from that location by logging-in. In step 120 the individual seeking remote access to the central computer and network will log-in in the normally accepted fashion. For instance, the individual will establish contact with the central computer and can present his or her identifying code and password. It is to be understood, of course, that the present invention can be used with any type of log-in procedure, and is not limited to a log-in procedure which uses an identifier and passcode. Further, it should be noted that once a location is registered and approved, as in steps 100 and 110 explained above, the individual need not register that location each time he or she wishes to log-in from that location. On the contrary, the central computer can store the registered and

approved location for future use. In other words, steps 100 and 110 need not be repeated each time the method of the present invention is to be utilized. It may be, however, that re-registration of locations will be required on the basis of some pre-selected criteria, and thus steps 100 and 110 will need to be repeated. For instance, re-registration of a location may be required after a certain period of time has elapsed, after a certain number of log-ins from that location have occurred, after a certain total number of system log-ins have occurred, or any other similar criterion.

In step 130, once the central computer is contacted by an attempted log-in, the central computer will identify on the basis of at least one parameter who the individual attempting to log-in purports to be and will activate the location device associated with that individual. In other words, if the central computer determines that the parameters of the identifier and password submitted in the log-in are associated with a computer user named "Tom", then the computer will activate the location device associated with "Tom" and which "Tom" carries around with him. It is to be understood, of course, that identification of the location device to be activated can be accomplished by any method and on the basis of any parameters which assure that the proper location device will be activated. For instance, parameters used in the log-in and subsequent activation may be on the basis of voice recognition, body heat signature, retinal scan, fingerprint scan, and/or visual observation, etc.

Further, actual activation of the location device can be carried out by any method, as long as the locating device is functionally activated. For instance, activation can be accomplished though radio signals, electrical signals, and/or infrared signals. Preferably the location device will be activated through a medium separate from that which the individual is using to log-in to the central computer. That is, for example, if the individual attempting to log-in is doing so over the Internet, the locating device can be activated through the use of satellite relays.

Upon activation, in step 140, the locating device transmits a location signal. Transmission of the location signal can be by any medium which ensures that the location signal is received by the central computer. For example, the location signal can be transmitted via airwave and relayed by satellite, or

through land-line using the Internet as a relay. The location signal itself can be any type of signal which is capable of carrying the location data and of being transmitted and received. For instance the signal can be radio wave, infrared, or even microwave. Preferably the location signal is broadcast as a radio wave in either a digital or analog format.

In step 150, the broadcast location signal is received by the central computer and a determination of the location of the locating device is made. In order to make the determination, the location signal may act as a homing beacon or may contain location data (coordinates). If the location signal acts as a homing beacon for the location of the location device, the central computer can determine the location of the locating device. If the locating signal contains location data, that is, the actual location (coordinates) of the locating device, then the location device itself can determine its own location. Either way, position detection will need to be accomplished and it is acceptable that any such position detection method or system be utilized. Preferably, the Global Positioning System is used.

Upon a determination of the location of the locating device, in step 160 the central computer decides if the locating device's location is at, or within a pre-determined proximity of, a pre-registered location. If the location is determined to be valid, log-in will be completed. If the location is not valid, log-in will be terminated. This decision step, then, determines whether access will be granted or denied. If the log-in is allowed to be completed, in step 170 the individual logging-in may then access the data files of the central computer. If the log-in is not allowed, in step 180 the connection is terminated and the central computer can generate appropriate messages to the appropriate parties that an unauthorized log-in was attempted.

In the case where the log-in is allowed because the locating device was determined to be at a pre-registered location, periodic updates of the location of the locating device may be accomplished. This ensures that the locating device stays with the individual who has logged-in, and can also act as a way of checking the original determination of the location of the locating device. Further, if any discrepancies occur in the subsequent updates, the central computer can terminate or restrict access. Lastly, an initial log-in from an authorized site can be used to

fine-tune the location's coordinates, if necessary, so that the system can be more accurate.

It should be noted that the central computer may also at any time send a message to the individual identified in step 130 that he or she has been identified as attempting to log-in and/or has been granted access to log-in. Thus if the individual identified in step 130 is at a pre-registered location, but is in fact not logging-in to the central computer, that individual can notify the appropriate personnel and access to the unauthorized individual in fact logging-in can be denied and/or terminated. Messages may be sent in any fashion which will reach the authorized individual identified in step 130. For instance, a message may be sent via telephone, pager, priority e-mail, etc.

Referring to Figure 2, transmission of the location signal is shown. In this example, the central computer 1 communicates with remote computer 2 via communication medium 4, and with location device 3 via communication medium 6. Thus, when an individual attempts to log-in to the central computer 1 using remote computer 2, the central computer 1 sends an activation signal by communication medium 6 to the location device 3. Communication medium 6 uses satellite system 5 for relay of communication. In response, location device 3 sends location signal 7 via communication medium 6 to central computer 1.

It should be noted that other information can be sent along with the location signal. For instance, information which might be sent might include a "time stamp". Such a "time stamp" could be utilized as an assurance that the location signal is being sent from the location indicated by it. The central computer could be synchronized to the GPS atomic clock and determinations of how long the location signal took to transmit could be made. Also, for instance, a passcode for the location device could be sent. A separate passcode for the location device would ensure that the proper location device was transmitting the location signal.

Thus, as can be seen from the foregoing description, an additional layer of computer security can be added to present computer security systems through the use of the present invention. Further, implementation of the present invention would require only nominal system adjustments.

In the foregoing description, the method and apparatus of the present invention have been described with reference to a specific example. It is to be understood and expected that variations in the principles of the method and apparatus herein disclosed may be made by one skilled in the art and it is intended that such modifications, changes, and substitutions are to be included within the scope of the present invention as set forth in the appended claims. The specification and the drawings are accordingly to be regarded in an illustrative rather than in a restrictive sense.

Claims:

1. A method for enhancing computer security using a location device, comprising the steps of:

registering at least one remote log-in location for a computer network;

registering a log-in contact to the computer network;

commanding activation of the location device upon establishment of the log-in contact;

receiving a location signal from the location device;

determining a location of the location device on the basis of the received location signal; and

determining whether the location of the location device is an authorized location with reference to the registered information that identifies the at least one authorized remote log-in location.

2. The method according to claim 1, further comprising the step of:

approving the registration of the at least one remote log-in location.

3. The method according to claim 1, further comprising the step of:

identifying the location device to be activated upon at least one parameter contained in the log-in contact.

4. The method according to claim 1, further comprising the step of:

determining an update of the location of the location device.

5. The method according to claim 1, further comprising the step of:

sending a message to an individual to whom the location device is identified as belonging.

6. The method according to claim 1, wherein activation of the location device is accomplished by radio wave.

7. The method according to claim 1, wherein the transmitted location signal may contain a plurality of data.

8. The method according to claim 7, wherein the plurality of data are location coordinates derived from a Global Positioning System.

9. The method according to claim 1, wherein the transmitted location signal contains a "time stamp".

10. The method according to claim 1, wherein access to the computer network is granted if the location of the location device matches the at least one remote registered log-in location.

11. The method according to claim 1, wherein access to the computer network is denied if the location of the location device does not match the at least one remote registered log-in location.

12. A method for enhancing computer security using a location device, comprising the steps of:

storing information identifying at least one authorized remote log-in location for log-in to a computer;

establishing a log-in contact with the computer;

activating transmission of a locating signal from the location device upon the log-in contact;

determining a location of the location device on the basis of the locating signal; and

determining whether the location of the locating device corresponds to the at least one remote log-in location.

13. The method according to claim 12, further comprising the step of:

securing authorization for the storing of the at least one remote log-in location.

14. The method according to claim 12, further comprising the step of:

identifying the location device from which the location signal is to be activated upon at least one parameter contained in the log-in contact.

15. The method according to claim 12, further comprising the step of:

determining an update of the location of the location device.

16. The method according to claim 12, further comprising the step of:

sending a message to an individual to whom the location device is identified as belonging.

17. The method according to claim 12, wherein activation of the location device is accomplished by radio wave.

18. The method according to claim 12, wherein the transmitted location signal may contain a plurality of data.

19. The method according to claim 18, wherein the plurality of data are location coordinates derived from a Global Positioning System.

20. The method according to claim 12, wherein the transmitted location signal contains a "time stamp".

21. The method according to claim 12, wherein computer access is granted if the location of the location device matches the at least one authorized remote log-in location.

22. The method according to claim 12, wherein computer access is denied if the location of the location device does not match the at least one authorized remote log-in location.

23. A method for enhancing computer security using a location device, comprising the steps of:

receiving a log-in contact;

commanding activation of the location device upon receipt of the log-in contact;

determining a location of the location device on the basis of a received location signal; and

determining whether the location of the location device corresponds to an authorized remote log-in location.

24. The method according to claim 23, further comprising the step of:

storing information identifying at least one authorized remote log-in location for log-in to a computer.

25. The method according to claim 24, further comprising the step of:

securing authorization for the storing of the at least one remote log-in location.

26. The method according to claim 23, further comprising the step of:

identifying the location device to be activated upon at least one parameter contained in the log-in contact.

27. The method according to claim 23, further comprising the step of:

determining an update of the location of the location device.

28. The method according to claim 23, further comprising the step of:

sending a message to an individual to whom the location device is identified as belonging.

29. The method according to claim 23, wherein activation of the location device is accomplished by radio wave.

30. The method according to claim 23, wherein the transmitted location signal may contain a plurality of data.

31. The method according to claim 30, wherein the plurality of data are location coordinates derived from a Global Positioning System.

32. The method according to claim 23, wherein the transmitted location signal contains a "time stamp".

33. The method according to claim 23, wherein computer access is granted if the location of the location device matches the authorized remote log-in location.

34. The method according to claim 23, wherein computer access is denied if the location of the location device does not match the authorized remote log-in location.

35. An apparatus for enhancing computer security using a location device, comprising:

a central computer;

means for receiving a location signal sent from the location device to the central computer, the location signal containing at least a location of the location device,

wherein access of the central computer is determined on the basis of the location of the location device matching a pre-registered access location.

36. The apparatus according to claim 35, further comprising:

means for determining the location of the locating device.

37. The apparatus according to claim 36, further comprising:

a means for communicating between the central computer and a remote station.

38. An apparatus for enhancing computer security using a location device, comprising:

a memory storing at least one authorized remote log-in location information;

a means for allowing a remote log-in contact;

an activator activating transmission of a location signal from the location device;

a receiver receiving the transmission of the location signal;

a means for determining a location of the location device on the basis of the transmitted location signal;

a central computer which determines whether the location of the location device is an authorized location with reference to the stored at least one authorized remote log-in location information.

FIG. 1

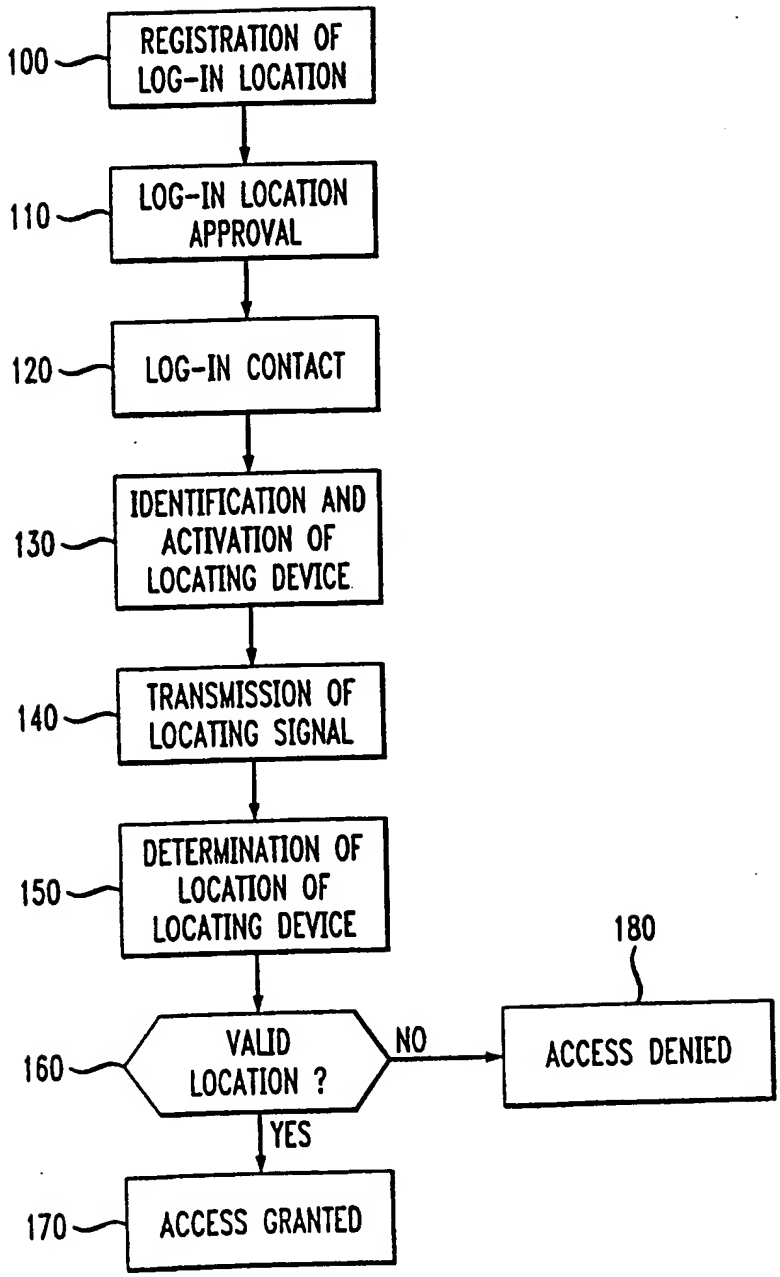
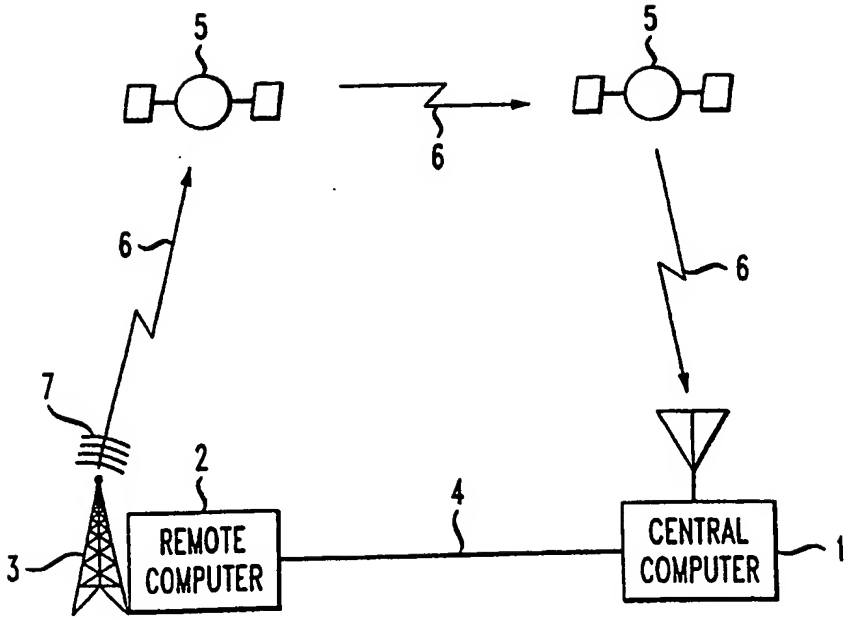

100
REGISTRATION OF LOG-IN LOCATION
110
LOG-IN LOCATION APPROVAL
120
LOG-IN CONTACT
130
IDENTIFICATION AND ACTIVATION OF LOCATING DEVICE
140
TRANSMISSION OF LOCATING SIGNAL
150
DETERMINATION OF LOCATION OF LOCATING DEVICE
160
VALID LOCATION ?
NO
180
ACCESS DENIED
YES
170
ACCESS GRANTED

FIG. 2



INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 99/05025

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 13341 A (INTERNATIONAL SERIES RESEARCH INC.) 10 April 1997 see page 10, line 29 - page 12, line 18 see page 15, line 12 - line 32 see page 45, line 13 - line 31; figures 1,3A,3B,4-6	1-3, 6-12,14, 17-24, 29-38
X	US 4 962 449 A (SCHLESINGER) 9 October 1990 see column 3, line 11 - line 34 see column 3, line 46 - column 4, line 18; figure 1	1-3,5, 10-12, 14,16, 21-24, 26,28, 33-38

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 July 1999	12/07/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Taylor, P

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 99/05025

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 93 21581 A (SECURE COMPUTING CORP.) 28 October 1993 see page 7, line 31 - page 8, line 23 see page 40, line 32 - page 43, line 25; figures 29-33	1-3,5-7, 10-12, 14, 16-18, 21-24, 26, 28-30, 33-38

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/US 99/05025

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9713341 A	10-04-1997	US 5757916 A	26-05-1998
		AU 7392196 A	28-04-1997
		CA 2233962 A	10-04-1997
		EP 0880839 A	02-12-1998
US 4962449 A	09-10-1990	NONE	
WO 9321581 A	28-10-1993	US 5276735 A	04-01-1994
		AT 154150 T	15-06-1997
		AU 4284793 A	18-11-1993
		AU 678937 B	12-06-1997
		AU 5081196 A	18-07-1996
		CA 2118246 A	28-10-1993
		DE 69311331 D	10-07-1997
		DE 69311331 T	30-10-1997
		DK 636259 T	07-07-1997
		EP 0636259 A	01-02-1995
		EP 0737907 A	16-10-1996
		JP 7505970 T	29-06-1995
		US 5502766 A	26-03-1996
		US 5499297 A	12-03-1996